Selected Vulnerabilities Report

# **Executive Summary**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S. No** | **Affected Asset i.e. IP/URL/Application etc** | **Observation/ Vulnerability title** | **CVE/CWE** | **Control Objective #** | **Control Name #** | **Audit Requirement #** | **Severity** | **Recommendation** | **Reference** | **New or Repeat observation** |
| 1 | N/A | Broken Access Control | CVE-2023-22515 / CWE-284 | N/A | N/A | N/A | N/A | 1. Assign only the necessary permissions based on user roles, and regularly review and update these permissions to prevent unauthorized access. 2. Conduct all access control checks on the server side to ensure users cannot bypass restrictions through client-side manipulation or direct API calls. 3. Use unpredictable URL patterns and ensure that API endpoints validate and verify user permissions for each request to prevent unauthorized access. 4. Continuously monitor access logs for anomalies and conduct regular security audits to detect and address any vulnerabilities in access control mechanisms. | https://cwe.mitre.org/data/definitions/284.html | N/A |
| 2 | N/A | Cryptographic Failures | CVE-2021-23841 / CWE-327 | N/A | N/A | N/A | N/A | 1. Use strong and up-to-date encryption algorithms to protect sensitive data. 2. Ensure encryption keys are stored securely and managed properly. 3. Regularly update cryptographic libraries to mitigate known vulnerabilities. 4. Educate developers on best practices for implementing encryption. | https://owasp.org/Top10/A02\_2021-Cryptographic\_Failures/ | N/A |

# **Vulnerability: Broken Access Control**

|  |  |
| --- | --- |
| **Affected Asset:**  N/A |  |
| **Vulnerability Title:**  Broken Access Control |  |
| **Business Impact:**  A Broken Access Control vulnerability can expose a company to unauthorized access to sensitive data, including customer details and proprietary business information, leading to significant data breaches. The financial impact can be immense, with costs for incident response, potential fines for non-compliance with regulations like GDPR or CCPA, and revenue loss due to diminished customer trust. Legal consequences include regulatory scrutiny, potential lawsuits, and compensation claims. Additionally, the company's reputation may suffer from erosion of customer trust, negative media attention, and a tarnished brand image. Finally, operational disruptions may occur as resources are diverted to address the breach and enhance security measures. |  |
| **Detailed observation:**  Broken Access Control occurs when an application fails to enforce proper restrictions on what authenticated users can access or perform within the system. This vulnerability arises when the application does not adequately verify whether a user has the appropriate permissions to access a specific resource or execute certain actions. For example, a user might manipulate URL parameters or API requests to gain access to administrative functions or sensitive data that should be restricted. This could involve direct object reference (accessing resources via predictable URLs) or bypassing authorization checks entirely. |  |
| **CVE/CWE:**  CVE-2023-22515 / CWE-284 |  |
| **Proof of Concept:** |  |
| **Vulnerable Points:**  N/A |  |
| **Recommendation:**  1. Assign only the necessary permissions based on user roles, and regularly review and update these permissions to prevent unauthorized access. 2. Conduct all access control checks on the server side to ensure users cannot bypass restrictions through client-side manipulation or direct API calls. 3. Use unpredictable URL patterns and ensure that API endpoints validate and verify user permissions for each request to prevent unauthorized access. 4. Continuously monitor access logs for anomalies and conduct regular security audits to detect and address any vulnerabilities in access control mechanisms. |  |
| **Reference:**  https://cwe.mitre.org/data/definitions/284.html |  |
| **New or Repeat observation:**  N/A |  |

# **Vulnerability: Cryptographic Failures**

|  |  |
| --- | --- |
| **Affected Asset:**  N/A |  |
| **Vulnerability Title:**  Cryptographic Failures |  |
| **Business Impact:**  Cryptographic failures can lead to exposure of sensitive data and weaken the security posture of a company. The financial impact can include costs related to data breaches, non-compliance fines, and revenue loss due to damaged reputation. Legal repercussions might involve regulatory actions and lawsuits. Operational disruptions may occur as organizations need to implement stronger encryption practices and possibly compensate affected parties. |  |
| **Detailed observation:**  This vulnerability occurs when data is not protected through adequate encryption methods, or when weak encryption algorithms are used. Examples include using deprecated cryptographic functions, not properly encrypting sensitive data at rest or in transit, and failing to securely store encryption keys. |  |
| **CVE/CWE:**  CVE-2021-23841 / CWE-327 |  |
| **Proof of Concept:** |  |
| **Vulnerable Points:**  N/A |  |
| **Recommendation:**  1. Use strong and up-to-date encryption algorithms to protect sensitive data. 2. Ensure encryption keys are stored securely and managed properly. 3. Regularly update cryptographic libraries to mitigate known vulnerabilities. 4. Educate developers on best practices for implementing encryption. |  |
| **Reference:**  https://owasp.org/Top10/A02\_2021-Cryptographic\_Failures/ |  |
| **New or Repeat observation:**  N/A |  |